# National Infrastructure Protection Center CyberNotes

*Issue #2002-17* *August 26, 2002*

**CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.**

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

## *Bugs, Holes & Patches*

The following table provides a summary of software vulnerabilities identified between August 7 and August 21, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| America OnLine[1] | Windows 95/98/ME/ NT 4.0/2000, XP | Instant Messenger 4.4-4.7, 4.7.2480, 4.8.2646, 4.8.2616 | A remote Denial of Service vulnerability exists due to the way special characters are handled. | No workaround or patch available at time of publishing. | Instant Messenger Special Character Remote Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Apache Software Foundation[2] | Unix | Tomcat 4.1, 4.1.3 beta, 4.1.9 beta | A Cross-Site Scripting vulnerability exists if a HTTP request is made for a JSP, which could let a malicious user execute arbitrary script code. | No workaround or patch available at time of publishing. | Tomcat Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |

[1] SecurityFocus, August 18, 2002.

[2] SecurityFocus, August 21, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Apache Software Foundation[3] | Windows NT 4.0/2000, XP, OS2 | Apache 2.0, 2.0.28 -BETA win32, 2.0.28 Beta, 2.0.28, 2.0.32-BETA win32, 2.0.32, 2.0.34 - BETA win32, 2.0.35-2.0.39 | A Directory Traversal vulnerability exists due to the failure to properly process the backslash character, which could let a remote malicious user obtain sensitive and a local malicious user execute arbitrary code if the cgi-bin directory is escaped. | Upgrade available at: http://www.apache.org/dist/httpd/ | Apache Backslash Directory Traversal<br>CVE Names: CAN-2002-0661, CAN-2002-0665 | Medium/ **High**<br>**(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. There is no exploit code required.<br>Vulnerability has appeared in the press and other public media. |
| Apache Software Foundation[4] | Windows NT 4.0/2000, XP | Apache 2.0, 2.0.28 -BETA win32, 2.0.28 Beta, 2.0.28, 2.0.32 - BETA win32, 2.0.32, 2.0.34 - BETA win32, 2.0.35-2.0.39 | Two path disclosure vulnerabilities exist: a vulnerability exists in the multiview type map negotiation when a specially crafted URL request is appended with .var, which could let a remote malicious user obtain sensitive information; and a vulnerability exists if the server fails to invoke a script, which could let a malicious user obtain sensitive information. | Upgrade available at: http://www.apache.org/dist/httpd/ | Apache Path Disclosure<br>CVE Name: CAN-2002-0654 | Medium | Bug discussed in newsgroups and websites. Multiview type map vulnerability can be exploited via a web browser. There is no exploit code required for the script vulnerability. |
| BlueFace Software[5] | Windows 95/98/NT 4.0/2000, XP | Falcon Web Server 2.0.0.1021 SSL Edition, 2.0.0.1021, 2.0.0.1020, 2.0.0.1009 | A Cross-Site Scripting vulnerability exists due to the lack of input sanitation in the error message output, which could let a malicious user execute arbitrary HTML and script code. | No workaround or patch available at time of publishing. | Falcon Web Server Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Cafelog[6] | Multiple | b2 2.6 pre4 | Multiple vulnerabilities exist in the WebLog Tool due to improper initialization of variables, which could let a malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | b2 WebLog Tool Multiple Vulnerabilities | **High** | Bug discussed in newsgroups and websites. |

[3] Apache Software Foundation, August 9, 2002.
[4] SecurityFocus, August 16, 2002.
[5] Bugtraq, August 8, 2002.
[6] Bugtraq, August 13, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Cisco Systems[7] | Windows, MacOS X 10.1.x, Unix | VPN Client 3.5.1 for Windows, Solaris, Mac OS X, Linux, 3.5.2 for Solaris, Mac OS X, Linux | Several remote Denial of Service vulnerabilities exist because Internet Key Exchange (IKE) implementations do not properly handle IKE response packets; and a buffer overflow vulnerability exists when malformed IKE packets are sent to the client, which could let a remote malicious user execute arbitrary code. | Customers may obtain upgrades through their regular channels, such as the Cisco's Software Center:<br>http://www.cisco.com/kobayashi/sw-center/ | VPN Client Multiple IKE Packet Vulnerabilities | Low/**High**<br>**(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. |
| Citrix[8] | Windows NT 4.0 | MetaFrame for Windows NT 4.0 TSE 1.8 | A remote Denial of Service vulnerability exists when a malicious user connects to the server using custom-crafted Java ICA files. | No workaround or patch available at time of publishing. | Metaframe Remote Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Coxco Support[9] | Windows 95/98/ME/ NT 4.0/2000, XP | Midicart ASP, Midicart ASP Maxi, Midicart ASP Plus | A vulnerability exists in the 'midicart.mdb' file due to a lack of access control, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Midicart ASP Remote Customer Information Retrieval | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Debian / RedHat[10] | Unix | Interchange 4.8.1-4.8.5 | A vulnerability exists due to the placement of the 'doc' folder, which could let a malicious user obtain sensitive information. | **RedHat:**<br>http://ftp.interchange.redhat.com/interchange/4.8/rpm/<br>**Debian:**<br>http://security.debian.org/pool/updates/main/i/interchange/ | Interchange Arbitrary File Read | Medium | Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. |
| Francisco Burzi/ Post Nuke Development Team[11] | Unix | PHP-Nuke 5.0-5.6; PostNuke Development Team PostNuke 0.62- 0.64, 0.70, 0.71, 0.703 | A Cross-Site Scripting vulnerability exists in the Private Messaging module, which could let a malicious user execute arbitrary HTML or JavaScript code. | No workaround or patch available at time of publishing. | PHP-Nuke Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| FreeBSD[12] | Unix | FreeBSD 4.0-4.6, 4.1.1-4.5-Stable, 4.1.1–4.3-Release, 4.5-4.6-Release | A buffer overflow vulnerability exists in the accept(2), getsockname(2), and getpeername(2) system calls, and in vesa(4) due to the assumption that a given argument was always a positive integer, which could let a malicious user obtain sensitive information or elevated privileges. | Patch available at:<br>ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:38/signed-error.patch | FreeBSD Signed Integer Buffer Overflow | Medium | Bug discussed in newsgroups and websites. |

[7] Cisco Security Advisory, August 12, 2002.
[8] SecurityFocus, August 11, 2002.
[9] Bugtraq, August 7, 2002.
[10] Debian Security Advisory, DSA 150-1, August 13, 2002.
[11] Bugtraq, August 15, 2002.
[12] FreeBSD Security Advisory, FreeBSD-SA-02:38, August 18, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Gateway[13] | Unix | GS-400 | A vulnerability exists because a default vendor password is used on all of their servers and is unchangeable via the administrative interface, which could let a remote malicious user obtain unauthorized root access. | Gateway will be contacting all GS-400 customers for instructions on returning their system. Since this server is unsupported, a fix will not be released. | GS-400 Server Default Administrator Password | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| GoAhead Software[14] | Windows 95/98/NT 4.0,<br>Unix | GoAhead WebServer 2.1 | A buffer overflow vulnerability exists, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | GoAhead WebServer Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Google[15] | Multiple | Google Toolbar 1.1.60 | A Denial of Service vulnerability exists when the Google Toolbar receives a search query. | No workaround or patch available at time of publishing. | Google Toolbar Denial of Service | Low | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Hewlett Packard Systems[16] | Unix | HP Secure OS Software for Linux 1.0 | A vulnerability exists in the 'tlcompadd' command due to insufficient Mandatory Access Control (MAC) restrictions, which could let a malicious user obtain unauthorized access to files. | Patch available at:<br>http://itrc.hp.com<br>Patch HPTL_00028 | HP Secure OS Software for Linux TLCompAdd MAC Restrictions | Medium | Bug discussed in newsgroups and websites. |
| Hewlett Packard Systems[17] | Unix | HP Secure OS software for Linux 1.0 | A vulnerability exists in the 'ptrace' and 'ioctl' kernel calls, which could let a malicious user obtain unauthorized access to data. | Patches available at:<br>http://itrc.hp.com<br>Patch HPTL_00025,<br>Patch HPTL_00026,<br>Patch HPTL_00027 | HP Secure OS For Linux PTrace / IOCTL Unauthorized Access | Medium | Bug discussed in newsgroups and websites. |
| Hewlett Packard Systems[18] | Unix | HP-UX (VVOS) 11.0 4 | A vulnerability exists in the passwd program, which could let a malicious user obtain elevated privileges and potentially administrative access. | Patch available at:<br>http://itrc.hp.com<br>PHCO_27373 | HP-UX VVOS Unspecified Local Passwd | Medium/ **High**<br>**(High if administrative access is obtained)** | Bug discussed in newsgroups and websites. |
| Hewlett Packard Systems[19] | Unix | Virtual Vault 4.0, 4.5, 4.6 | A stack corruption vulnerability exists in the TGA Daemon, which could let a malicious user obtain elevated privileges and potentially administrative access. | Patches available at:<br>http://itrc.hp.com<br>PHSS_27499,<br>PHSS_27500,<br>PHSS_27501 | Virtual Vault TGA Stack Corruption | Medium/ **High**<br>**(High if administrative access is obtained)** | Bug discussed in newsgroups and websites. |

[13] Bugtraq, August 14, 2002.
[14] Securiteam, August 14, 2002.
[15] Bugtraq, August 15, 2002.
[16] Hewlett-Packard Company Security Bulletin, HPSBTL0208-059, August 13, 2002.
[17] Hewlett-Packard Company Security Bulletin, HPSBTL0208-058, August 13, 2002.
[18] Hewlett-Packard Company Security Bulletin, HPSBUX0208-0210, August 14, 2002.
[19] Hewlett-Packard Company Security Bulletin, HPSBUX0208-0211, August 14, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Ilia Alshanetsky[20] | Unix | FUDForum 1.2.8, 1.9.8, 2.0.2 | Several vulnerabilities exist: a vulnerability exists in the 'tmp_view.php' script due to a failure to check the path of the requested file, which could let a malicious user obtain sensitive information; a vulnerability exists in the 'admbrowse.php' script because access is allowed to files and directories outside of FUDForum directories, which could let a malicious user add, delete, and modify data; and a vulnerability exists because SQL code may be inserted into requests, which could let a malicious user execute arbitrary SQL code. | Upgrade available at:<br>http://fud.prohost.org/download/FUDforum2_20020712.tar.gz | FUDForum Multiple Vulnerabilities | Medium/ **High**<br>**(High if arbitrary SQL is executed)** | Bug discussed in newsgroups and websites. Proof of Concept exploits have been published for the 'tmp_view.php' & 'admbrowse.php' script vulnerabilities. |
| isdn4linux[21] | Unix | isdn4linux 3.1 pre1 | A format string vulnerability exists in the 'ipppd' utility, which could let a malicious user execute arbitrary code with root privileges. | **SuSE:**<br>ftp://ftp.suse.com/pub/suse/ | ISDN4Linux IPPPD Utility Format String | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Kerio[22] | Windows NT | Mailserver 5.0, 5.1, 5.1.1 | Multiple vulnerabilities exist: numerous Denial of Service vulnerabilities exist when a malicious user sends multiple "SYN" packets to the server; and several cross-site scripting vulnerabilities exist in the web mail component, which could let a malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | MailServer Multiple Denial of Service & Cross-Site Scripting Vulnerabilities | Low/**High**<br>**(High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| l2tpd[23] | Unix | l2tpd 0.62-0.67 | A vulnerability exists in the rand() function because random numbers are generated without seeding the random generator, which could let a remote malicious user predict tunnel and session IDs to perform a man-in-the-middle attack. | Upgrade available at:<br>http://www.l2tpd.org/downloads/l2tpd-0.68.tar.gz<br>**Debian:**<br>http://security.debian.org/pool/updates/main/l/l2tpd/l2/ | L2TPD Weak Random Number Generator | Medium | Bug discussed in newsgroups and websites. |

[20] Bugtraq, August 19, 2002.
[21] SuSE Security Announcement, SuSE-SA:2002:030, August 12, 2002.
[22] Securiteam, August 21, 2002.
[23] Debian Security Advisory, DSA 152-1, August 13, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Leszek Krupinski[24] | Multiple | L-Forum 2.4 .0 | Two vulnerabilities exist: a vulnerability exists in 'search.php' due to insufficient filtering of the 'From,' E-mail,' and 'Subject' fields of a message post, which could let a remote malicious user execute arbitrary SQL commands; and a vulnerability exists in the file upload function because uploads are allowed to occur without checking the four global variables for information about an upload, which could let al malicious user download any file on the server. | Patch available at:<br>http://sourceforge.net/tracker/download.php?group_id=53716&atid=471343&file_id=26687&aid=579278 | L-Forum Multiple Vulnerabilities | Medium/ **High**<br>**(High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| LG Electronics[25] | Multiple | LR3001f 4.0,<br>LR3100p 1.50,<br>LR3100p 1.30 | A Denial of Service vulnerability exists when a remote malicious user sends a stream of data to port 23/TCP (port 80/TCP on some models). | No workaround or patch available at time of publishing. | LR Series WAN Router Denial of Service | Low | Bug discussed in newsgroups and websites. |
| LG Electronics[26] | Multiple | LR3001f 4.0,<br>LR3001f 4.57,<br>LR3100p 1.50,<br>LR3100p 1.30 | A buffer overflow vulnerability exists in the authentication challenge when a stream of data is sent in the password field, which could let a malicious user cause a Denial of Service. | No workaround or patch available at time of publishing. | LR Series Telnet Daemon Buffer Overflow | Low | Bug discussed in newsgroups and websites. |
| Linex Kernel[27] | Unix | kernel 2.4.18 pre-1-8, 2.4.18, 2.4.19 -pre1-6 | Several security issues exist: security issues exist in the stradis, rio500, se401, usbvideo, and apm devices, which could let a malicious user obtain elevated privileges; and vulnerabilities exist in components of the procfs virtual filesystem because kernel memory may be exposed, which could let a malicious user obtain elevated privileges. | Upgrade available at:<br>ftp://updates.redhat.com/7.3/en/os/ | Linux Kernel Multiple Security Issues | Medium | Bug discussed in newsgroups and websites. |
| Macromedia[28] | Windows 95/98/ME/ NT 4.0/2000, XP | Flash 4.0 r12, 5.0 r50, 5.0, 6.0, 6.0.29.0, 6.0.40.0, 6.0.47.0 | A Denial of Service vulnerability exists when a malicious user sends a Flash Shockwave (.SWF) movie file that contains a malformed body. | No workaround or patch available at time of publishing. | Flash Malformed SWF Denial of Service | Low | Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published. |

[24] Bugtraq, August 13, 2002.
[25] Securiteam, August 21, 2002.
[26] Bugtraq, August 21, 2002.
[27] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:158-09, August 20, 2002.
[28] Bugtraq, August 11, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **Macromedia[29]**<br>***Vulnerability appears in Press[30]*** | **Windows 95/98/ME/NT 4.0/2000, XP, Unix** | **Flash 5.0, 6.0, 6.0.29.0** | **A buffer overflow vulnerability exists in Flash Shockwave movie files (.SWF) due to insufficient bounds checking of headers, which could let a remote malicious user execute arbitrary code.** | **Upgrades available at:**<br>**http://www.macromedia.com/shockwave/download/frameset.fhtml?P1_Prod_Version=ShockwaveFlash**<br>**Flash 5.0r50 (Linux)**<br>**http://www.macromedia.com/go/getflashplayer/** | **Flash Malformed Header Buffer Overflow** | **High** | **Bug discussed in newsgroups and websites.**<br>***Vulnerability has appeared in the press and other public media.*** |
| Mantis[31] | Unix | Mantis 0.15.3-0.15.12, 0.16.0, 0.16.1, 0.17.0-0.17.3 | A vulnerability exists in 'summary_graph_ functions.php' because the path to the include file is not properly validated, which could let a remote malicious user execute arbitrary code. | Upgrade available at:<br>http://sourceforge.net/project/showfiles.php?group_id=14963 | Mantis JPGraph Remote Command Execution | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Mantis[32] | Unix | Mantis 0.15.3-0.15.12, 0.16.0, 0.16.1, 0.17.0-0.17.2 | A vulnerability exists in the 'account_update.php' component, which could let a malicious user obtain elevated privileges. | Upgrade available at:<br>http://sourceforge.net/project/showfiles.php?group_id=14963 | Mantis Account Update | Medium | Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. |
| Mantis[33] | Unix | Mantis 0.15.3-0.15.12, 0.16.0, 0.16.1, 0.17.0-0.17.3 | A vulnerability exists in the 'View Bugs' page because it does not verify access to the defined project, which could let a malicious user obtain unauthorized access to restricted projects. | Upgrade available at:<br>http://sourceforge.net/project/showfiles.php?group_id=14963 | Mantis Unauthorized Project Viewing | Medium | Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. |
| Mantis[34] | Unix | Mantis 0.16.0, 0.17.0-0.17.3 | A vulnerability exists in the 'print_all_bug_page.php' script because the 'limit_reporters' option is not implemented, which could let a malicious user obtain sensitive information. | Upgrade available at:<br>http://sourceforge.net/project/showfiles.php?group_id=14963 | Mantis Limit Reporters Option Bypass | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Mantis[35] | Unix | Mantis 0.17.0-0.17.3 | A vulnerability exists because the path to the include file is not properly validated, which could let a remote malicious user execute arbitrary code. | Upgrade available at:<br>http://sourceforge.net/project/showfiles.php?group_id=14963 | Mantis Remote File Include Command Execution | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |

[29] eEye Digital Security Advisory, August 8, 2002.
[30] CNET News.com, August 12, 2002.
[31] Mantis Advisory, 2002-04, August 19, 2002.
[32] Mantis Advisory, 2002-01, August 19, 2002.
[33] Mantis Advisory, 2002-03, August 19, 2002.
[34] Mantis Advisory, 2002-02, August 19, 2002.
[35] Mantis Advisory, 2002-05, August 19, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft[36] | Windows NT 4.0/2000 | 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 Server SP1&2, 2000 Terminal Services, 2000 Terminal Services SP1&2 | A vulnerability exists because the NTFS system event auditing system fails to properly record filesystem events when hard links are involved, which could let a malicious user access restricted files. | For Microsoft Windows 2000 Advanced Server SP2, Datacenter Server SP2, Professional SP2 and 2000 Server SP2, apply the latest Windows 2000 Service Pack (SP3 or later), available at: http://www.microsoft.com/windows2000/downloads/ | Windows NTFS Incorrect Hard Link Auditing<br>CVE Name: CAN-2002-0725 | Medium | Bug discussed in newsgroups and websites. |
| Microsoft[37] | Windows NT 4.0/2000 | Data Engine 1.0, 2000, SQL Server 7.0, SQL Server 7.0 SP1-4, SQL Server 2000, SQL Server 2000 SP1&2 | A vulnerability exists in some of the jobs that the Agent executes due to weak permissions, which could let a malicious user obtain elevated privileges. | No workaround or patch available at time of publishing. | Microsoft SQL Agent Jobs Privilege Elevation | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Microsoft[38] | Windows NT 4.0/2000 | Data Engine 1.0, SQL 2000, SQL Server 7.0. SQL Server 7.0 SP1-4, SQL Server 2000, SQL Server 2000 SP1&2, | A vulnerability exists in some of the extended stored procedures due to weak permissions, which could let a malicious user obtain unauthorized administrator privileges. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-043.asp | Microsoft SQL Server Extended Stored Procedure Privilege Elevation<br>CVE Name: CAN-2002-0721 | **High** | Bug discussed in newsgroups and websites. |

[36] @stake Inc. Security Advisory, A081602-1, August 16, 2002.
[37] NGSSoftware Insight Security Research Advisory, #NISR15002002B, August 15, 2002.
[38] Microsoft Security Bulletin, MS02-043, August 14, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft[39] | Windows NT 4.0/2000, XP | 2000 Advanced Server, 2000 Advanced Server SP1-3, 2000 Datacenter Server, 2000 Datacenter Server SP1-3, 2000 Professional, 2000 Professional SP1-3, 2000 Server, 2000 Server SP1-3, 2000 Terminal Services, 2000 Terminal Services SP1-3 | A vulnerability exists in the Network Connection Manager (NCM) because it is possible for an unprivileged user to configure the handler routine, which could let a malicious user obtain elevated privileges. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-042.asp | Windows 2000 Network Connection Manager Privilege Elevation<br>CVE Name: CAN-2002-0720 | Medium | Bug discussed in newsgroups and websites.<br>Vulnerability has appeared in the press and other public media. |
| Microsoft[40] | Windows | DirectX Files Viewer | A buffer overflow vulnerability exists in the "File" parameter of the Microsoft DirectX Files Viewer ActiveX control, which could let a remote malicious user execute arbitrary code. | This has been fixed in the most recent service pack for Internet Explorer (6.0 SP1) and will be fixed in Windows 2000 SP3 and Windows XP SP1. S. http://windowsupdate.microsoft.com/default.htm | DirectX Files Viewer Remote Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| Microsoft[41] | Windows 95/98/ME/ NT 4.0/2000 | Internet Explorer 4.0, 4.0.1, 4.0.1 SP2, 5.0, 5.0.1, 5.0.1 SP1&2, 5.5, 5.5 SP1&2, 6.0 | A vulnerability exists in a XML Datasource applet, which could let a malicious user view the contents of local files via a remote page. | No workaround or patch available at time of publishing. | Internet Explorer XML Datasource Applet | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[39] Microsoft Security Bulletin, MS02-042, August 14, 2002.
[40] Bugtraq, August 16, 2002.
[41] Securiteam, August 19, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft[42] | Windows | File Transfer Manager | Several vulnerabilities exist: a buffer overflow vulnerability exists in the Microsoft File Transfer Manager (FTM) ActiveX control used for secure file delivery to/from Microsoft prior to June 2002, which could let a malicious user execute arbitrary code; and the File Transfer Manager is vulnerable to man-in-the-middle attacks, which could let a malicious user upload/download any file. | Upgrade available at:<br>http://transfers.one.microsoft.com/ftm/install/HomeIE.asp | Microsoft File Transfer Manager ActiveX Control Buffer Overflow & Arbitrary File Upload | Medium/ High<br>(High if arbitrary code is executed) | Bug discussed in newsgroups and websites.<br>Vulnerability has appeared in the press and other public media. |
| **Microsoft[43]**<br>***Microsoft issues patch[44]*** | **Windows 95/98/ME/NT 4.0/2000** | **Internet Explorer 5.0.1, 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0; Proxy Server 2.0; ISA Server 2000** | **A buffer overflow vulnerability exists in the component that parses gopher replies, which could let a remote malicious user execute arbitrary code.** | **Frequently asked questions regarding this vulnerability and the patch can be found at:**<br>**http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-027.asp**<br>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-047.asp | **Multiple Microsoft Product Gopher Client Buffer Overflows**<br>**CVE Names: CAN-2002-0371,** ***CAN-2002-0646*** | **High** | **Bug discussed in newsgroups and websites.** ***Exploit script has been published.***<br>**Vulnerability has appeared in the press and other public media.** |
| Microsoft[45] | Windows 95/98/ME/ NT 4.0/2000 | Internet Explorer 5.5, 5.5 SP1&2, 6.0 | A vulnerability exists in the 'Web Folder" feature, which could let a remote malicious user execute arbitrary HTML or script code. | No workaround or patch available at time of publishing. | Internet Explorer Web Folder HTML Injection | High | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| **Microsoft[46]**<br>***Microsoft issues patch[47]*** | **Windows 95/98/ME/ NT 4.0/2000** | **Internet Explorer 5.5, 5.5 SP1&2, 6.0** | **A vulnerability exists because the object property of embedded WebBrowser controls is not subject to the Cross-Domain security checks, which could let a malicious user obtain elevated privileges, steal arbitrary cookies, or execute arbitrary commands.** | ***Frequently asked questions regarding this vulnerability and the patch can be found at:***<br>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-047.asp | **Internet Explorer Universal Cross Domain Scripting**<br>***CVE Name: CAN-2002-0723*** | **Medium/ High**<br>**(High if arbitrary code can be executed)** | **Bug discussed in newsgroups and websites. Exploits have been published.**<br>**Vulnerability has appeared in the press and other public media.** |

[42] Bugtraq, August 18, 2002.
[43] Microsoft Security Bulletin, MS02-027 V2.0, June 14, 2002.
[44] Microsoft Security Bulletin, MS02-047, August 22, 2002.
[45] NTBugtraq, August 15, 2002.
[46] Thor Larholm, PivX, Security Advisory, TL#003, July 10, 2002.
[47] Microsoft Security Bulletin, MS02-047, August 22, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft[48] | Windows 95/98/ME/ NT 4.0/2000 | Internet Explorer 5.5, 5.5 SP1&2, 6.0 | Multiple vulnerabilities exist: a buffer overflow vulnerability exists because an obsolete ActiveX control used for certain types of text formatting contains an unchecked buffer, which could let a malicious user execute arbitrary code; a vulnerability exists due to the way HTML directives are handled that display XML data, which could let a malicious user read contents from websites that users had access; a vulnerability exists that involves how the origin of a file in the File Downlaod Dialogue box is represented, which could let a malicious user fool a user into downloading a file from an untrusted source; and a new variant of the "Cross-Site Scripting in Local HTML Resource" vulnerability exists that was originally discussed in Microsoft Security Bulletin MS02-023, which could let a malicious user execute arbitrary HTML or script code. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-047.asp | Internet Explorer Multiple Vulnerabilities<br>CVE Names: CAN-2002-0691, CAN-2002-0647, CAN-2002-0648, CAN-2002-0722 | Medium/ **High**<br>**(High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. |
| Microsoft[49] | Windows 98/ME/NT 4.0/2000 | Internet Explorer 6.0 | A vulnerability exists when an e-mail is sent with an attached HTM file that contains malicious PHP script referenced as an iframe source, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Internet Explorer Script Execution | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Microsoft[50] | Windows 98/ME/NT 4.0/2000 | Internet Explorer 6.0 | A vulnerability exists in the java logging feature because it may provide a storage place for malicious code, which could let a malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Microsoft Internet Explorer Java Logging Executable Code | **High** | Bug discussed in newsgroups and websites. |
| Microsoft[51] | Windows 95/98/ME/ NT 4.0/2000, XP | TSAC ActiveX Control | A buffer overflow vulnerability exists due to an unchecked buffer in the code that processes one of the input parameters, which could let a remote malicious user execute arbitrary code. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-046.asp | TSAC ActiveX Control Buffer Overflow<br>CVE Name: CAN-2002-0726 | **High** | Bug discussed in newsgroups and websites. |

[48] Microsoft Security Bulletin, MS02-047, August 22, 2002.
[49] Bugtraq, August 13, 2002.
[50] Bugtraq, August 17, 2002.
[51] Microsoft Security Bulletin, MS02-046, August 22, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **Microsoft**[52]<br>*Microsoft issues patch*[53] | **Office 2000, XP** | *OfficeWeb Compon-ents 2000, 2002, Project 2000, 2002* | **A vulnerability exists in the 'Paste' method of the 'Range' object and the 'Copy' method of the 'Cell' object, which could let a malicious user gain control over the clipboard even when the 'Allow paste operations via script' security feature in IE is disabled.** | *Frequently asked questions regarding this vulnerability and the patch can be found at:*<br>*http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-044.asp* | **Office Web Component Clipboard Information Disclosure**<br>*CVE Name: CAN-2002-0861* | **Medium** | **Bug discussed in newsgroups and websites. Exploit has been published.** *Vulnerability has appeared in the press and other public media.* |
| **Microsoft**[54]<br>*Microsoft issues patch*[55] | **Windows 2000, XP** | *OfficeWeb Compon-ents 2000, 2002, Project 2000, 2002* | **A vulnerability exists in the 'LoadText' method of the Range object, which could let a malicious user read the content of any known local file.** | *Frequently asked questions regarding this vulnerability and the patch can be found at:*<br>*http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-044.asp* | **Office Web Component Local File**<br>*CVE Name: CAN-2002-0860* | **Medium** | **Bug discussed in newsgroups and websites. Exploit has been published.** *Vulnerability has appeared in the press and other public media.* |
| **Microsoft**[56]<br>*Microsoft issues patch*[57] | **Windows 2000, XP** | *OfficeWeb Compon-ents 2000, 2002, Project 2002, Project Server 2002* | **Numerous vulnerabilities exist: a vulnerability exists in the Chart component because the 'Load' method does not perform security checks on the assigned URL, which could let a malicious user obtain sensitive information; a vulnerability exists in the Spreadsheet component in OWC10 because the 'XMLURL' property blindly follows redirections, which could let a malicious user obtain sensitive information; and a vulnerability exists in the DataSourceControl component in OWC10 because the 'ConnectionFile' property does not perform security checks on the assigned URL, which could let a malicious user obtain sensitive information.** | *Frequently asked questions regarding this vulnerability and the patch can be found at:*<br>*http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-044.asp* | **Office Web Components Multiple Vulnera-bilities**<br>*CVE Name: CAN-2002-0860* | **Medium** | **Bug discussed in newsgroups and websites. Exploits have been published.**<br>**Vulnera-bilities have appeared in the press and other public media.** |

[52] GreyMagic Security Advisory, GM#007-IE, April 8, 2002.
[53] Microsoft Security Bulletin, MS02-044 V1.1, August 22, 2002.
[54] GreyMagic Security Advisory, GM#006-IE, April 8, 2002.
[55] Microsoft Security Bulletin, MS02-044 V1.1, August 22, 2002.
[56] GreyMagic Security Advisory, GM#008-IE, April 8, 2002.
[57] Microsoft Security Bulletin, MS02-044 V1.1, August 22, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **Microsoft**[58]<br>***Microsoft issues patch***[59] | **Windows 2000, XP** | ***OfficeWeb Components 2000, 2002, Project 2002, Project Server 2002*** | **A vulnerability exists in the spreadsheet component when the 'setTimeout' method of the window object is used through the '=HOST()' formula, which could let a malicious user execute arbitrary script code even when Active Scripting has been disabled.** | ***Frequently asked questions regarding this vulnerability and the patch can be found at:***<br>***http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-044.asp*** | **Office Web Components Active Script Execution**<br>***CVE Name: CAN-2002-0727*** | **High** | **Bug discussed in newsgroups and websites. Exploit has been published.**<br>**Vulnerability has appeared in the press and other public media.** |
| Microsoft[60] | Windows 2000 | Windows 2000 Terminal Services, Terminal Services SP1-SP3 | A vulnerability exists because the screensaver will not automatically lock the session if the client window is minimized, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Terminal Services Inactive Console Screensaver Lock Failure | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Microsoft[61] | Windows NT 4.0/2000, XP | Windows NT 4.0 Server, NT 4.0 Workstation, NT 4.0 Server, Terminal Server Edition, 2000 Professional, 2000 Server, 2000 Advanced Server, XP Professional | A Denial of Service vulnerability exists when a malicious user sends a specially crafted SMB_COM_ TRANSACTION packet. | Frequently asked questions regarding this vulnerability and the patch can be found at:<br>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-045.asp | Network Share Provider SMB Request Buffer Denial of Service<br>CVE Name: CAN-2002-0724 | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft[62] | Windows XP | Windows XP Home, XP Professional, Internet Explorer 6.0 | A vulnerability exists in the Microsoft Help and Support Center HCP URI handler, which could let a remote malicious user delete files on another user's computer. | This issue is planned to be addressed in Microsoft Windows XP SP1. | Microsoft Windows XP HCP URI Handler Abuse | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[58] GreyMagic Security Advisory, GM#005-IE, April 8, 2002.
[59] Microsoft Security Bulletin, MS02-044 V1.1, August 22, 2002.
[60] Bugtraq, August 21, 2002.
[61] Microsoft Security Bulletin, MS02-045, August 22, 2002.
[62] Bugtraq, August 15, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Mozilla[63] | Unix | Bonsai 1.3 | Multiple vulnerabilities exist: several Cross-Site Scripting vulnerabilities exist due to a lack of stripping of tags from user input, which could let a malicious user execute arbitrary script code; and a path disclosure vulnerability exists when a malformed request is submitted, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Bonsai Multiple Cross Site Scripting & Path Disclosure Vulnerabilities | Medium/ **High**<br>**(High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published. |
| Multiple Vendors[64] | Windows 95/98/ME/ NT 4.0/2000 | AT&T WinVNC 3.3 x, 3.3.3 R9, 3.3.3 r7 & Previous; TightVNC 1.2.0-1.2.5; Tridia TridiaVNC 1.5, 1.5.1, 1.5.2, 1.5.4 | A vulnerability exists in the graphical user interface elements, which could let a malicious user send arbitrary messages to the privilege process and possibly execute arbitrary code. | No workaround or patch available at time of publishing. | Multiple Vendor VNC Products Messaging API | Medium/ **High**<br>**(High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. A tool that exploits this vulnerability has been published. |
| Multiple Vendors[65] | Multiple | Compaq Wireless LAN WL310; Proxim Orinoco Residential Gateway RG-1000 | A vulnerability exists because a system identification string is used as the default SNMP community string, which could let a remote malicious user view and modify sensitive system configuration information. | No workaround or patch available at time of publishing. | Multiple Vendor SNMP Community String<br>CVE Name: CAN-2002-0812 | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Multiple Vendors[66] | Unix | Debian Linux 3.0; SGI IRIX 6.5.15-6.5.17 | A vulnerability exists in the FAM's group handling, which could let a malicious user obtain sensitive information. | **Debian:**<br>http://security.debian.org/pool/updates/main/f/fam/ | FAM Directory File Listing | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[63] Bugtraq, August 19, 2002.
[64] Bugtraq, August 20, 2002.
[65] Foundstone Labs Advisory, 080902-APIL, August 9, 2002.
[66] Debian Security Advisory, DSA 154-1, August 15, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Multiple Vendors[67] | Windows 95/98/MT/ NT 4.0/2000, Unix | GNU Privacy Guard 1.0-1.0.7; IETF OpenPGP RFC 2440; Network Associates PGP 5.0 i, 5.0 Linux, PGP 5.0, 5.5.3 i for Windows, 5.5.3 i, 5.5.5, 6.0.2i, 6.0.2, 6.5 Linux, 6.5.1 i for Unix, 6.5.1i, 6.5.3i for Windows, 6.5.3, 6.5.8, 7.0, 7.0.3, 7.0.4, 7.1, 7.1.1, 7.0.3 | A vulnerability exists in programs that use the OpenPGP format, which could let a remote malicious user obtain portions of encrypted messages using a "chosen-ciphertext" attack. | No workaround or patch available at time of publishing. | Multiple Vendor Ciphertext Message Disclosure | Medium | Bug discussed in newsgroups and websites. |
| Multiple Vendors[68, 69] | Unix | Caldera OpenUnix 8.0, UnixWare 7, 7.1.0, 7.1.1; Compaq Tru64 4.0g, 4.0f, 5.0a, 5.1a, 5.1; HP HP-UX 10.10, 10.20, 10.24, 11.0, 11.11; IBM AIX 4.3.3, 5.1; Sun Solaris 2.5.1, 2.6, 7.0, 8.0, 9.0; Xi Graphics DeXtop 2.1 | A buffer overflow vulnerability exists in the _TT_CREATE_FILE procedure, which could let a remote malicious user execute arbitrary code or cause a Denial of Service. | **Sun Microsystems, Inc:**<br>http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert%2F46366<br>**Hewlett Packard:**<br>ftp://ttdb1:ttdb1@hprc.external.hp.com/rpc.ttdbserver.2.tar.gz<br>**Xi Graphics:**<br>ftp://ftp.xig.com/pub/updates/dextop/2.1/DEX2100.016.tar.gz<br>**IBM:**<br>ftp.software.ibm.com/aix/efixes/security/. | Multiple Vendor CDE ToolTalk Database Server Buffer Overflow<br>CVE Name: CAN-2002-0679 | Low/**High**<br>**(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. |

[67] Bugtraq, August 12, 2002.
[68] Entercept Ricochet Advisory, August 12, 2002.
[69] CERT® Advisory, CA-2002-26, August 12, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| MySQL AB[70] | Windows | MySQL 3.20.32 a, 3.22.26-3.22.30, 3.22.32, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.23-3.23.31, 3.23.34, 3.23.36-3.23.52 | Multiple vulnerabilities exist: a vulnerability exists because root login is allowed without a password, which could let a malicious user obtain elevated privileges; a vulnerability exists because the 'bind-address' configuration directive is not enabled by default, which could let a remote malicious user obtain unauthorized access; and a vulnerability exists because most logging is disabled by default, which could let malicious actions go undetected. | No workaround or patch available at time of publishing. | MySQL Multiple Vulnerabilities | Medium | Bug discussed in newsgroups and websites. Exploit script has been published for the null password vulnerability. There is no exploit code required for the 'bind-address' configuration & disabled logging vulnerabilities. |
| MyWeb Server[71] | Windows 95/98/ME/ NT 4.0/2000 | MyWeb Server 1.0.2 | Several vulnerabilities exist: a remote buffer overflow vulnerability exists when an overly long search parameter is submitted to the search engine, which could let a remote malicious user execute arbitrary code or cause a Denial of Service; a vulnerability exists when an oversized HTTP request is received, which could let a malicious user execute arbitrary code; and a vulnerability exists when an invalid directory is requested, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | MyWebServer Multiple Vulnerabilities | Low/ Medium/ **High**<br>**(Medium if sensitive information is obtained and High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. There is no exploit code required for the invalid directory vulnerability. Exploit script has been published. |
| nCipher[72] | Multiple | nForce, nShield | A vulnerability exists in the cryptographic library because invalid signatures may not be detected, which could let a malicious user tamper with or forge messages. | Contact nCipher Support for details on obtaining the updated software. | nCipher Message Signature Verification | Medium | Bug discussed in newsgroups and websites. |
| Network Associates[73] | Windows 95/98/ME/ NT 4.0/2000, MacOS 9.0 | PGP Freeware 7.0.3 | A buffer overflow vulnerability exists in the Internet Key Exchange (IKE) used by the VPN client when malformed IKE response packets are handled, which could let a malicious user execute arbitrary code or cause a Denial of Service. | No workaround or patch available at time of publishing. | PGPFreeware Malformed IKE Response Buffer Overflow | Low/**High**<br>**(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. |

[70] Bugtraq, August 18, 2002.
[71] D4rkGr3y Advisory, August 14, 2002.
[72] nCipher Security Advisory No. 5, August 19, 2002.
[73] CERT Vulnerability Note VU#287771, August 11, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Novell[74] | Multiple | Netware 5.1, 5.1 SP4, 6.0, 6.0 SP1 | A vulnerability exists due to the way HTTP requests are handled when Perl is used as a handler, which could let a malicious user obtain unauthorized access. | Upgrade available at: http://support.novell.com/servlet/filedownload/ftf/perl5002.exe/ | NetWare Buffer Overflow & Scripting Vulnerability | Medium | Bug discussed in newsgroups and websites. |
| Novell[75] | Multiple | Netware 5.1, 5.1 SP4, 6.0, 6.0 SP1 | Two vulnerabilities exist: a vulnerability exists when Perl is used as a handler, which could let a remote malicious user arbitrary Perl code via POST; and a Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information. | Upgrade available at: http://support.novell.com/servlet/filedownload/ftf/perl5002.exe/ | NetWare Remote Perl Handler Vulnerabilities | **High** | Bug discussed in newsgroups and websites. |
| Novell[76] | Multiple | Netware 5.1, 6.0; Small Business Suite 5.1, 6.0 | Several vulnerabilities exist: a Directory Traversal vulnerability exists in the NetBasic Scripting Server, which could let a remote malicious user obtain sensitive information; and a buffer overflow vulnerability exists in the Novell NetBasic Scripting Server (NSN) due to insufficient bounds checking of module requests, which could let a remote malicious user execute arbitrary code. | Patch available at: http://support.novell.com/servlet/filedownload/ftf/nscript1.exe | NetBasic Scripting Server Directory Traversal & Module Name Buffer Overflow | Medium/ **High**<br>**(High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. |
| Novell[77] | Multiple | Netware 6.0 SP2 | A vulnerability exists in RconJ because access can be obtained without a password, which could let a remote malicious user obtain unauthorized access. | Update available at: http://support.novell.com/servlet/filedownload/ftf/nw6rconj2a.exe/ | NetWare RConsoleJ Secure IP Login | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| OpenBSD[78] | Unix | OpenBSD 3.0, 3.1 | A buffer overflow vulnerability exists in the select(2) function due to insufficient boundary checks in the select call, which could let a malicious user overwrite kernel memory and execute arbitrary code. | Patch available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.1/common/014_scarg.patch | OpenBSD select() Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |

[74] Security Alert, NOVL-2002-2963297, August 20, 2002.
[75] Security Alert, NOVL- 2002-2963307, August 20, 2002.
[76] Security Alert, NOVL- 2002-2963297, August 20, 2002.
[77] NOVL-2002-2963349, August 21, 2002.
[78] OpenBSD Security Advisory, August 11, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Oracle Corporation[79] | Multiple | Oracle 9i Application Server 1.0.2.2. 1.0.2.1s, 1.0.2, 9.0.2 | Cross-Site Scripting vulnerabilities exist in the sample OJSP scripts due to insufficient santization of HTML tags in text fields in forms, which could let a malicious user execute arbitrary script code. | The vendor advises administrators to remove the OJSP demo scripts. This may be accomplished by removing the following JSP files:<br>/ora9ias/j2ee/OC4J_Demos/applications/ojspdemos/ojspdemos-web/basic/simple<br>and<br>/ora9ias/j2ee/OC4J_Demos/applications/ojspdemos/ojspdemos-web/basic/hellouser | Oracle 9iAS OJSP Demo Scripts Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. |
| Oracle Corporation[80] | Multiple | Oracle8i 8.1.5-8.1.7.1, Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Release 2 9.2 2, 9.2.1 | A format string vulnerability exists in the Listener Control utility (LSNRCTL) because the default configuration does not protect against unauthenticated access and control, which could let a remote malicious user obtain control over the Listener Control utility. | Patch available at:<br>http://metalink.oracle.com<br>(reference Bug Number 2395416) | Oracle Net Listener Format String | Medium | Bug discussed in newsgroups and websites. |
| Oracle Corporation[81] | Multiple | Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.1 | A remote Denial of Service vulnerability exists when a malicious user sends a malformed debugging request to the server. | Patch available at:<br>http://metalink.oracle.com<br>(Reference Bug Number 2467947) | Oracle Listener Remote Denial of Service<br>CVE Name: CAN-2002-0856 | Low | Bug discussed in newsgroups and websites.<br>Vulnerability has appeared in the press and other public media. |
| Organic PHP[82] | Multiple | PHP-Affiliate 1.0 | A vulnerability exists in the 'details.php' script due to improper input validation, which could let a remote malicious user modify other affiliate's account details. | No workaround or patch available at time of publishing. | PHP-Affiliate 'Details.PHP' Authentication Bypassing | Medium | Bug discussed in newsgroups and websites. |

[79] Oracle Security Alert #41, August 14, 2002.

[80] NGSSoftware Insight Security Research Advisory, #NISR14082002, August 14, 2002.

[81] Internet Security Systems Security Bulletin, August 13, 2002.

[82] Bugtraq, August 15, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Pingtel[83] | Multiple | Xpressa 1.2.5, 1.2.7.4, 1.2.8, 2.0, 2.0.1 | Multiple vulnerabilities exist which affect all aspects of the phone's operation. A vulnerability exists in IP phones because registration information is sent via the HTTP protocol, which could let a malicious user obtain sensitive information; and a vulnerability exists because predictable values are used for the Call-ID and CSeq parameters in SIP communications, which could let a malicious user inject arbitrary data into a valid communication stream. | No workaround or patch available at time of publishing. | Xpressa Phone Multiple Vulnerabilities | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Postgre SQL[84] | Multiple | Postgre SQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2 | A buffer overflow vulnerability exists in the in cash_words() function because overly long queries are not handled properly, which could let a malicious user execute arbitrary code. | Upgrade available at: http://www.postgresql.org/ | PostgreSQL cash_words Buffer Overflow | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| Postgre SQL[85] | Multiple | Postgre SQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2, 7.2.1 | A buffer overflow vulnerability exists in the repeat() function, which could let a malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | PostgreSQL Repeat Function Buffer Overflow | High | Bug discussed in newsgroups and websites. |
| Postgre SQL[86] | Multiple | Postgre SQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2, 7.2.1 | A buffer overflow vulnerability exists in the lpad() and rpad() functions because overly large integer arguments are handled properly, which could let a malicious user cause a Denial of Service. This vulnerability only affects data bases that were created using special international encodings | No workaround or patch available at time of publishing. | PostgreSQL lpad() & rpad() functions Buffer Overflow | Low | Bug discussed in newsgroups and websites. |
| SGI[87] | Unix | IRIX 6.5.13-6.5.16 | A vulnerability exists when an Origin 3000 system is upgraded from a version prior to the 6.5.13 release to a release between versions 6.5.13 and 6.5.16 because a change was made in the MAC address for the base Ethernet, which could let a malicious user bypass access controls. | Upgrade to IRIX 6.5.17 available at: http://support.sgi.com/colls/patches/tools/relstream/index.html | IRIX MAC Address Changing | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |

[83] Sys-Security Group Security Advisory, August 20, 2002.
[84] @(#) Mordred Labs Advisory, 0x0001, August 19, 2002.
[85] @(#)Mordred Labs Advisory 0x0003, August 20, 2002.
[86] @(#) Mordred Labs Advisory 0x0004, August 20, 2002.
[87] SGI Security Advisory, 20020805-01-I, August 14, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| SGI[88] | Unix | IRIX 6.5-6.5.16 | A vulnerability exists in the Bulk Data Service, which could let a remote malicious user obtain sensitive information. | Patch available at: ftp://patches.sgi.com/support/free/security/patches/ patch 4713 | SGI Irix Bulk Data Services Arbitrary File Disclosure<br>CVE Name: CAN-2002-0632 | Medium | Bug discussed in newsgroups and websites. |
| SGI[89] | Unix | IRIX 6.5-6.5.16 | A vulnerability exists in the FTP server when the PASV mode is in use because predictable PASV mode port numbers are selected, which could let a remote malicious user hijack data connections. | Upgrade to IRIX 6.5.17 available at: http://support.sgi.com/colls/patches/tools/relstream/index.html | IRIX ftpd PASV Mode Hijacking | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Stephen Ball[90] | Multiple | File Manager 1.5 | Several vulnerabilities exist: a Directory Traversal vulnerability exists in the 'source.php' script, which could let a remote malicious user obtain sensitive information and a vulnerability exists in the 'userlist.cgi' file, which could let an unauthorized malicious user without admin privileges manipulate accounts. | No workaround or patch available at time of publishing. | File Manager Directory Traversal & Privilege Elevation | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Sublimation.org [91] | Unix | SCPOnly 2.3, 2.4 | A vulnerability exists in the default installation due to insufficient access controls on the .ssh subdirectory, which could let a remote malicious user execute arbitrary commands. | **Workaround:** Each user with SCPOnly as his or her shell must have an immutable home directory and .ssh subdirectory to prevent a user from using ssh config parameters to undermine the shell. | SCPOnly SSH Environment Shell Escaping | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Sun Microsystems, Inc.[92] | Multiple | Cobalt RaQ 4.0 | A vulnerability exists in the /usr/lib/authenticate utility, which could let a malicious user obtain elevated privileges. | No workaround or patch available at time of publishing. | Cobalt RaQ Elevated Privileges | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Sun Microsystems, Inc.[93] | Unix | PatchPro 2.0 | A vulnerability exists because temporary files are created insecurely, which could let a malicious user obtain sensitive information. | Patch available at: http://sunsolve.sun.com Patch 113176-01 | PatchPro Insecure Temporary File | Medium | Bug discussed in newsgroups and websites. |

[88] SGI Security Advisory, 20020804-01-P, August 12, 2002.
[89] SGI Security Advisory, 20020305-03-I, August 14, 2002.
[90] Bugtraq, August 21, 2002.
[91] Bugtraq, August 19, 2002.
[92] SecurityFocus, August 21, 2002.
[93] Sun Alert, 113176, August 21, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Sun Micro-systems, Inc.[94] | Unix | Solaris 2.4, 2.5, 2.5.1_x86, 2.5.1, 2.6_x86, 2.6, 7.0_x86, 7.0, 8.0_x86, 8.0 | A buffer overflow vulnerability exists in the XView library, which could let a malicious user execute arbitrary code. | Patches available at:<br>http://sunsolve.sun.com<br>Patch 107375-02,<br>Patch 107374-02,<br>Patch 111627-01,<br>Patch 111626-01 | Sun XView Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| Tiny Software[95] | Windows NT | Personal Firewall 3.0, 3.0.5, 3.0.6 | A Denial of Service vulnerability exists when a malicious user browses the Agents Logs while the system is being portscanned. | No workaround or patch available at time of publishing. | Tiny Personal Firewall Log File Viewing Denial Of Service | Low/**High**<br>**(High if DDoS best practices not in place)** | Bug discussed in newsgroups and websites. |
| Toma hawk Technol-ogies[96] | Windows NT 4.0/2000 | SteelArrow Web Application Server 4.1 | Multiple buffer overflow vulnerabilities exist: a vulnerability exists when an overly long value is supplied in the Cookie HTTP header, which could let a malicious user execute arbitrary code; a vulnerably exists when an overly long request is made for a .aro extension, which could let a malicious user execute arbitrary code; and a vulnerability exists when processing requests for .aro files coded with the 'Chunked Encoding' mechanism, which could let a malicious user execute arbitrary code. | Patch available at:<br>http://www.steelarrow.com | SteelArrow Multiple Buffer Overflow Vulnerabilities | **High** | Bug discussed in newsgroups and websites. |
| University of Kansas[97] | Multiple | Lynx 2.8.2 rel.1- 2.8.4 rel.1, 2.8.5 dev.8 | A vulnerability exists when carriage return and line feed (CRLF) characters are included in the commandline, which could let a malicious user make scripts that use Lynx for downloading files from the wrong site on a web server with multiple virtual hosts. | Patch available at:<br>ftp://lynx.isc.org/lynx2.8.4/patches/lynx2.8.4rel.1c.patch | Lynx Command Line URL CRLF Injection | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |

[94] SecurityFocus, August 15, 2002.
[95] NSSI-Research Labs Security Advisory, NSSI-2002-tpfw, August 20, 2002.
[96] NGSSoftware Insight Security Research Advisory, #NISR19082002B, August 19, 2002.
[97] Bugtraq, August 19, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| W3C[98] | Multiple | CERN httpd 3.0 | A Cross-Site Scripting vulnerability exists in the httpd proxy due to the way URLs are displayed in error messages, which could let a malicious user execute arbitrary HTML or script code. | No workaround or patch available at time of publishing. | W3C CERN httpd Proxy Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| W3C[99] | Multiple | Jigsaw 2.2 | A Cross-Site Scripting vulnerability exists in the httpd proxy due to the way URLs are displayed in error messages, which could let a malicious user execute arbitrary HTML or script code. | Upgrade available at:<br>http://www.w3.org/Jigsaw/#Getting | Jigsaw Proxy Server Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| WebEasy Mail[100] | Windows NT | WebEasy Mail 3.4.2.2 | Multiple vulnerabilities exists: a format string vulnerability exists due to incorrect handling of user input by the SMTP service, which could let a malicious user cause a Denial of Service; and a vulnerability exists when authentication is attempted against the POP3 server because it is easy to determine if a username exists, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | WebEasyMail Multiple Vulnerabilities | Low/ Medium (Medium if sensitive information is obtained) | Bug discussed in newsgroups and websites. There is no exploit code required for the POP3 authentication vulnerability. |
| Webscript world[101] | Windows | Web Shop Manager 1.1 | A vulnerability exists due to improper validation of input to the search box, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Web Shop Manager Search Box Improper Validation | **High** | Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. |
| Xinetd[102, 103] | Unix | Xinetd 2.3.4-2.3.6 | A remote Denial of Service vulnerability exists when file descriptors are used to talk to xinetd due to a signal pipe leak. | **Xinetd:**<br>http://synack.net/xinetd/xinetd-2.3.7.tar.gz<br>**Debian:**<br>http://security.debian.org/pool/updates/main/x/xinetd/ | Xinetd Remote Denial of Service | Low | Bug discussed in newsgroups and websites. |

*"Risk" is defined by CyberNotes in the following manner:

**High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

[98] Bugtraq, August 11, 2002.
[99] Bugtraq, August 17, 2002.
[100] Securiteam, August 21, 2002.
[101] Bugtraq, August 15, 2002.
[102] Debian Security Advisory, DSA 151-1, August 13, 2002.
[103] Gentoo Linux Security Announcement, August 14, 2002.

**Medium** – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

**Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

## *Recent Exploit Scripts/Techniques*

The table below contains a representative sample of exploit scripts and How to Guides, identified between August 10 and August 22, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 29 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

| Date of Script (Reverse Chronological Order) | Script Name | Script Description |
|---|---|---|
| August 22, 2002 | Nessquick.zip | A pair of Perl scripts designed to assist in managing the output from Nessus scans that creates an alternate report format. These scripts help produce a report that lists all vulnerabilities and then enumerates each host that was found to contain that vulnerability. |
| **August 21, 2002** | **Raqfuck.sh** | **Exploit for the Cobalt RaQ Elevated Privileges vulnerability.** |
| August 20, 2002 | Ethereal-0.9.6.tar.gz | A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames. |
| August 20, 2002 | Holygrail.c | Script which exploits the Solaris Telnetd vulnerability. |
| August 20, 2002 | Mssql-jobs2.txt | Proof of concept SQL code for the Microsoft SQL Server 2000 "helper" service vulnerability. |
| August 20, 2002 | Sbofcoder.pl | Simple Bof Coder for Linux and BSD constructs Proof of Concept buffer overflow code by asking several questions about the vulnerability. |
| August 20, 2002 | Virus-writing-HOWTO-2002-08-15.tar.gz | The Linux Virus Writing HOW TO describes how to write parasitic file viruses which infect ELF executables on Linux/i386. |
| August 19, 2002 | Lynx-crlf.pl | Perl script which exploits the Lynx Command Line URL CRLF Injection vulnerability. |
| **August 18, 2002** | **Blowdoor01b.c** | **This is a Unix backdoor that contains a definable port, password, executable to run, process to show job, and logging facility.** |
| August 18, 2002 | Imapdog.pl | Perl script which exploits the IMAP4 RedHat and Slackware Linux vulnerability |
| **August 18, 2002** | **Mysqlfuck.c** | **Script which exploits the MySQL Null Root Password & Bind-Address Configuration vulnerability.** |
| August 18, 2002 | Pjam2.zip | A UDP packet flooder for Windows. |
| August 18, 2002 | Ultimaratiovegas.c | Script which exploits the IOS TFTP Buffer Overflow vulnerability. |

| Date of Script (Reverse Chronological Order) | Script Name | Script Description |
|---|---|---|
| August 16, 2002 | Mssql-esppu.txt | Proof of Concept SQL code for the Microsoft SQL Server 2000 helper service vulnerability. |
| **August 16, 2002** | **MWS_exp.pl** | **Perl script which exploits the MyWebServer Buffer Overflow vulnerability.** |
| **August 13, 2002** | **Helpme.pl** | **Perl script that exploits the Winhlp32.exe remote buffer overflow vulnerability.** |
| August 13, 2002 | Lcrzoex-4.13-src.tgz | A toolbox for network administrators and malicious users that contains over 200 functionalities using network library lcrzo. |
| August 13, 2002 | Mimedefang-2.17.tar.gz | A flexible MIME e-mail scanner. |
| August 13, 2002 | Nessus-1.2.4.tar.gz | Full featured remote security scanner for Linux, BSD, Solaris and some other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over 910 remote security checks. |
| August 13, 2002 | Sql2kx2.txt | Exploit for the Microsoft SQL Server 2000 buffer overflow vulnerability. |
| August 12, 2002 | Sql2kx.c | Script which exploits the Microsoft SQL Server 2000 buffer overflow vulnerability. |
| August 11, 2002 | Aveofattack.pdf | "A New Avenue of Attack: Event-Driven System Vulnerabilities" is a paper that provides technical details to security vulnerabilities in event-driven systems and relates them to Information Warfare. |
| August 11, 2002 | Nikto-1.20.tar.gz | A PERL open source web server scanner that supports SSL. |
| August 11, 2002 | Secvulnsineventdrivensys.pdf | " Security Vulnerabilities in Event-Driven Systems" is a paper that examines security vulnerabilities in event-driven systems. |
| August 10, 2002 | Centurion2.0a.tar.gz | Tool that checks for CGI scripts on remote servers for vulnerabilities such as: traversal bug, null byte, and incorrect filtering of meta characters. |
| August 10, 2002 | GOBBLES-own-ipppd.c | Script which exploits the ISDN4Linux IPPPD Utility Format String vulnerability. |
| August 10, 2002 | Int.exp.txt | Exploit for the RedHat Interchange Arbitrary File Read vulnerability. |
| August 10, 2002 | Shatter.html | A paper that paper presents a new generation of attacks against Microsoft Windows, and possibly other message-based Windowing systems which were unfixable at the time of writing. |
| August 10, 2002 | Shatter.zip | Proof-of-concept exploit that shows how vulnerable Win32 Messaging System is due to a failure to authenticate a message's source. |

## *Trends*

- **The Common Desktop Environment (CDE) ToolTalk RPC database server contains a buffer overflow vulnerability that could allow a remote malicious user to execute arbitrary code or cause a denial of service. For more information see "Bugs, Holes & Patches" Table and CERT® Advisory CA-2002-26, located at: http://www.cert.org/advisories/CA-2002-26.html.**
- **There has been an increase in Distributed Denial of Service (DDoS) attacks reported in the first seven months of 2002 over the number of DDoS attacks last year.**
- **The National Infrastructure Protection Center (NIPC) has issued an advisory to heighten the awareness of multiple buffer overflows in OpenSSL (Open Secure Sockets Layer). For more information, see NIPC Advisory 02-006, located at: http://www.nipc.gov/warnings/advisories/2002/02-006.htm.**
- **There has been an increase in scanning for the Apache Chunk Encoding Vulnerability and direct reports of exploitation have been received by CERT/CC. For more information see http://www.cert.org/current/current_activity.html#Apache.**

- **A warning has been issued by NIPC regarding a potential vulnerability in numerous versions of the open-source Apache Web Server Software. This vulnerability can allow remote access to the system and gives an intruder the ability to take control of the system and execute root level commands. NIPC considers this to be a significant threat due to the large installed base of Apache Servers, the potential for remote compromise, and the level of access granted by this vulnerability. For more information, see NIPC Advisory 02-005, located at: http://www.nipc.gov/warnings/advisories/2002/02-005.1.htm**
- **Numerous exploit scripts exist which exploit the Apache Chunked-Encoding Memory Corruption vulnerability.**

## *Viruses*

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

**BAT.Etimolod.A (Alias: BAT_ETIMOLOD.A) (Batch Worm):** This is a worm that spreads using the file-sharing software KaZaA. When it copies itself, it uses many file names in an attempt to trick other users into downloading and executing the worm. The worm also attempts to either delete system files on the C drive or format the C drive.

**BAT_MIGRATE.A (Alias: BAT.Migrate.A@mm) (Batch File Worm):** This batch file worm propagates by sending itself as an attachment in an e-mail with the following details:

- Subject: A Greeting Card For You
- Message Body: Coz you're special to me... :)
- Attachment: GREETING.CARD.BAT

It also spreads via Internet Relay Chat (IRC), DCC (Direct Client Connection) Send, and KaZaA, the peer-to-peer file application that allows users to share files over a network.

**BAT.Natay@mm (Alias: Trojan.BAT.KillAV.h) (Batch File Virus):** This is a DOS batch file which comes as an attachment to a Microsoft Outlook e-mail message. When it is run, it attempts to delete all antivirus files and create a VBS script to mail itself out. The e-mail message has the following characteristics:

- Subject: Happy National Day Singapore!
- Attachment: NationalDay2002.bat

**Godzilla (Aliases: VBS/Godzilla.A@m, I-Worm.Godzilla) (Visual Basic Script Worm):** This is a slow mass mailing worm. It activates by reading an infected e-mail message. Godzilla.A uses Outlook Express 5.0 to spread as HTML source in each e-mail from infected machine. To do this it saves its code in Update.hta in Windows Startup folder:

- C:\WINDOWS\START MENU\PROGRAMS\STARTUP\

so it will be executed next time when the system is restarted. The virus also saves itself in C:\Windows folder in a file Sign.html. By modifying the Windows registry:

- KKCU\Identities\DefaultUserID\Software\Microsoft\OutlookExpress\5.0\Signatures

it changes Outlook Express signature to use Sign.html. The worm code will be embedded in each outgoing e-mail message. If the date is October 10th, VBS/Godzilla.A shows a message box with a the following text:

- Have you danced with the devil in the moonlight ?

VBS/Godzilla.A@m also contains the following comment on the top of its code:

- I-Worm.Godzilla Coded by Zorro

**Prophecy.Worm (DOS Executable Worm):** This is a DOS executable that sends itself to all addresses in the Microsoft Outlook Address Book. The e-mail message has the following characteristics:

- Subject: I Finally Found it!
- Attachment: Prophecy.exe

The worm e-mails itself using a Visual Basic Script.

**TR/Bat.Dolomite (Alias: Bat/zq) (Batch File Virus):** This virus uses the file exchange P2P network KaZaA in order to trick unknowning users. If executed, will first be prompted to install the dolomite registry key. It then prompts a user to make a selection 1, 2, or 3.

**VBS_EDNAV.A (Alias: EDNAV) (Visual Basic Script Virus):** This destructive Visual Basic Script deletes files located at the desktop. It propagates by infecting VBS files and by sending copies of itself through e-mail using Microsoft Outlook. The e-mail it sends out has the following format:

- Subject: "System Administrator Notification"
- Attachment: %infected VBS file%

**VBS/LoveLet-DO (Aliases: VBS/LoveLetter@MM, VBS/LoveLetter.gen, I-Worm.LoveLetter) (Visual Basic Script Worm):** This worm arrives in an e-mail with the following characteristics:

- Subject line: fwd: Joke
- Attached file: Very Funny.vbs
- The e-mail contains no message text.

When the worm is first executed, it creates three copies of itself as C:\Windows\System\MSKernel32.vbs, C:\Windows\Win32DLL.vbs, and C:\Windows\System\Very Funny.vbs. The following two entries are added to the registry and point to the infected files MSKernel32.vbs and Win32DLL.vbs respectively:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL

This will run the worm when Windows starts up. If the file C:\Windows\System\WinFAT32.exe exists, then the Internet Explorer start page will be changed, via the registry setting:

- HKCU\Software\Microsoft\Internet Explorer\Main\Start Page

to one of the following four addresses:

- http://www.skyinet.net/~young1s/ HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw6587345gvsdf7679njbvYT/WIN-BUGSFIX.exe
- http://www.skyinet.net/~angelcat/ skladjflfdjghKJnwetryDGFikjUIyqwerWe546786324hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe
- http://www.skyinet.net/~koichi/ jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBdQZnmPOhfgER67b3Vbvg/WIN-BUGSFIX.exe
- http://www.skyinet.net/~chu/ sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUgqwerasdjhPhjasfdglkN Bhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-BUGSFIX.exe

If the file WIN-BUGSFIX.exe is downloaded from one of the above addresses, then the following entry is added to the registry and points to the downloaded file:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX

The Internet Explorer start page will then be set to a blank page. At the time of writing, the file WIN-BUGSFIX.exe is not available from any of the above addresses. The virus infects VBS, VBE, JS, JSE, CSS, WSH, SCT, HTA, JPG, JPEG, MP2, and MP3 files by overwriting their original contents with a copy of itself and adding a VBS extension, except in the case of VBS and VBE files. The worm searches for a mIRC installation and creates a new script.ini file in the mIRC folder. This script.ini file attempts to send the infected file, C:\Windows\System\Very Funny.vbs, to all users who join the current channel. The virus is sent to all contacts in the user's Windows address book in an e-mail message. An HTML file named, “Very Funny.HTM,” is created in the Windows system folder. This HTM file contains a VBScript that will not execute correctly.

**VBS.Natay (Visual Basic Script Virus):** This is a Visual Basic script virus that uses Microsoft Outlook to send a DOS Batch file. The virus creates a mail object to attach a DOS batch file to a message. The e-mail message has the following characteristics::

- Subject: Happy National Day Singapore!
- Message: Happy Birthday To Singaporeans!!!
- Attachment: NationalDay2002.bat

If the batch file is executed, it creates multiple copies of itself and a new Visual Basic script e-mailing worm. The batch file is detected as BAT.Natay@mm.

**VBS_ROKOL.A (Aliases: ROKOL.A, ROKOL) (Visual Basic Script Malware):** This malware propagates via e-mail. Upon execution, it drops an ORLOK.VBS file in the Windows System directory. Then it adds this registry entry so that it executes upon Windows startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run\ORLOK wscript.exe %systemdir%ORLOK.vbs

It also checks for the value of this registry key:

- HKEY_CURRENT_USER\software\ORLOK\mailed

If the value of the registry key does not exist, it uses Mail Application Programming Interface to send a copy of itself to all e-mail addresses listed in the infected system's Microsoft Outlook Address Book. The details of the e-mail the this malware arrives with are as follows:

- Subject: "I feel sick today!!!"
- Message Body: I am ORLOK.

After successfully mailing itself, it creates this registry entry and then sets its value to "1:"

- HKEY_CURRENT_USER\software\ORLOK\mailed

It also checks if a MANGE.COM file exists in the Windows System directory. If it does not find the file, it sets the Start Page of the infected system's Internet Explorer to this URL:

- http:\\membres.lycos.fr\aoteam\mange.com

The change downloads a MANGE.COM file from the URL when the user of the infected system opens Internet Explorer. If the file MANGE.COM file already exists, it copies MANGE.Com form the default Internet Explore download directory to the Windows System directory that executes MANGE.COM. The author of this malware may change the contents of theMANGE.COM file anytime. The malware also overwrites all files with the .VBS and .VBE extensions in the root directory of each drive and continuously runs an instance of the NOTEPAD.EXE application until the infected system eventually hangs and the user has to restart the system and lose unsaved data on running applications. The malware body contains these text strings:

- 'I am Orlok
- Orlok.08052002

**W32.Areq (Win32 Virus):** This is a virus that copies itself as:

- A:\Fotos.exe
- C:\Windows_.exe

It also attempts to perform several actions if it is executed as A:\Fotos.exe on any of these dates:

- August 30, 2001
- October 15, 2001
- November 15, 2001
- December 2, 2001

**W32.Axatak (Win32 Virus):** This is a password stealer that stores the stolen passwords in the file Axatak.is and then sends the file to the virus creator. The virus also allows unauthorized access to an infected computer on ports 8888 and 8889.

**W32/Duload.worm (Aliases: W32.HLLW.Yoof, W32/Duload-A, WORM_DULOAD.A) (Win32 Worm):** This worm is written in Visual Basic 6, and attempts to spread via KaZaA peer-to-peer file-sharing networks. This worm installs itself to %WinDir%\System as SYSTEMCONFIG.EXE (e.g. C:\Windows\System\systemconfig.exe). The following Registry keys are added to run the worm at subsequent system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Windows system Configure" = C:\WINDOWS\SYSTEM\SystemConfig.exe
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "Windows system Configure" = C:\WINDOWS\SYSTEM\SystemConfig.exe
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Windows system Configure" = C:\WINDOWS\SYSTEM\SystemConfig.exe

The worm copies itself into the following directory (creating it if necessary) %WinDir%\System\Media. Various filenames are used, designed to entice other KaZaA users to run the worm and various KaZaA settings are then modified by setting the following Registry keys:

- HKEY_CURRENT_USER\Software\Kazaa\LocalContent "Dir0" = C:\WINDOWS\SYSTEM\Media\
- HKEY_LOCAL_MACHINE\Software\Kazaa\CloudLoad “ShareDir" = C:\WINDOWS\SYSTEM\Media\
- HKEY_CURRENT_USER\Software\Kazaa\LocalContent "Dir1" = C:\WINDOWS\SYSTEM\Media\
- HKEY_CURRENT_USER\Software\Kazaa\LocalContent "Dir2" = 012345:C:\WINDOWS\SYSTEM\Media\
- HKEY_CURRENT_USER\Software\Kazaa\LocalContent "DisableSharing" = 0
- HKEY_CURRENT_USER\Software\Kazaa\Transfer "DlDir0" = 012345:C:\WINDOWS\SYSTEM\Media\
- HKEY_CURRENT_USER\Software\Kazaa\Transfer "DlDir1"= C:\WINDOWS\SYSTEM\Media\
- HKEY_CURRENT_USER\Software\Kazaa\Transfer "DlDir99" = 012345:C:\WINDOWS\SYSTEM\Media\

Additionally, the worm attempts to download an executable file from a specific URL. It attempts to download the file to C:\UNINSTALL.EXE, and if successful executes it. At the time of writing, this remote file was not available at the URL specified within the worm.

**W32.Golsys.14292 (Alias: W32.Nios.14292) (Win32 Virus):** This is a variant of W32.Golsys.8020; however, the virus size of this variant is 14,292 bytes. This virus infects Windows 32-bit executable files both on the local hard drive and on mapped drives. When W32.Golsys.14292 runs, it first copies itself as %system%\Netbios.exe, which it then runs as a service. It infects Windows 32-bit executable files on the local hard drive and on mapped drives by appending itself to the host files.

**W32.HLLP.Nedal (Win32 Virus):** This is a Visual Basic virus that copies itself to the Windows folder and infects all .exe files in that folder by prepending itself to them. When a file that is infected with W32.HLLP.Nedal runs, it executes the viral code and infects .exe files in the Windows folder. It then creates a file with the .wtc extension and executes that file. The virus also modifies the file %windir%\Win.ini by adding this text:

- [NYC-WTC-IN-KERNEL]
- OSAMA BL=TERROR IN USA

**W32.Hunch.E@mm (Alias: W32.HLLW.Dejas) (Win32 Worm):** This is a mass-mailing worm that sends itself to all addresses in the Microsoft Outlook Address Book. The e-mail message has the following characteristics:

- Subject:<blank>
- Message: Mensaje importante para <Name of the sender> en el archivo adjunto...
- Attachment:<This varies depending on the originating file name>

**W32.Mortag (Win32 Virus):** This is a password-stealing virus that is written in Visual Basic. When this virus is executed, it will display the a fake error message. It copies itself as “System%Wind32reg.dll.exe” and creates %System%\Winsck32.sys.txt. This file is where the virus will log keystrokes. The virus then sends the log file to the author of the worm using it's own SMTP engine. The virus copies itself as A:\MortalGame.html.exe. It also adds the value, “Win32reg.dll C:\Windows\System\Wind32reg.dll.exe” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

so that the virus runs every time that you start Windows.

**W32.Vig.Worm (Alias: W32/Toguivi, W32.HLLW.Vig, Win32.Vig, W32/Vig.worm) (Win32 Worm):** This worm writes itself to the root of all local and mapped drives. It also modifies the registry so that it runs whenever you start Windows. It is written in Visual Basic and is packed with UPX. When it runs, it does the following: It writes itself to the root of all local and mapped drives, including network drives. It writes itself to different file names, such as Viguito.exe, Pamela.exe, Juego.exe, and Tetris.exe, among others. All files are the same; each is 24,064 bytes in length. The worm also tries to create a file named \Windows\System\Dll32run.exe. This file name does not change from iteration to iteration. The path is hard-coded as "Windows\System;” the worm does not read the system folder settings. On systems with Windows installed in a different folder, this file is not created. The worm adds the value, “SystemCheck C:\Windows\System\DLL32RUN.exe” to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that it runs when you start Windows. It also changes the registered owner by modifying the value in:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RegisteredOwner to “Viguito Bufón”

W32.Vig.Worm also deletes C:\Windows\Regedit.exe. The path is hard-coded and is not dependent on a system variable. This file must be restored from a clean backup or reinstalled.

**W97M.Creutze (Aliases: Macro.Word97.Creutze, W97M/Creutze.A) (Word 97 Macro Virus):** This is a macro virus that infects the Normal.dot template when you open an infected document in Microsoft Word 97. After Normal.dot becomes infected, clean documents become infected when you close them. The viruses in this family all infect when documents are opened. Upon infection, W97M.Creutze renames the "This Document" module to "Creutzfeldt_Jakob." This macro virus tries to hide its activity by disabling Macro commands on the Tools menu. It also disables Microsoft Word macro security by setting the value data of Level to 1. in the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security

The virus also inserts ASCII art into infected documents.

**W97M.Maike (Word Macro Virus):** This virus infects documents by way of the Normal.dot template when a document is opened, closed, or saved. It also infects Normal.dot when Visual Basic code is viewed (Alt+F11) or macros are displayed (Alt+F8). Macro code is exported to and imported from the %system%\Maike.sys file. The macro will not infect documents on the 1st, 14th, or 28th of the month, but it will change the registry so that when the registered owner and organization are displayed, they appear as:

- Maike, you are the most beautiful girl in the world.

It does this by making several changes to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

The value data of “RegisteredOwner” is changed to “Maike you are.” The value data of “RegisteredOrganization” is changed to “the most beautiful.” The value data of “ProductId” is changed to “girl in the world.” You can reset these values to their original settings. In addition, when Word 2000 is installed, the macro resets security to the lowest level by setting the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security\Level

to a value of 1. The virus creates the key if it does not exist.

**WORM_HARAS .A (Alias: I-Worm.Generic, W32.Mylife.M@mm, W32.Mylife@mm) (Internet Worm):** This mass-mailing worm propagates via e-mail using Microsoft Outlook. It uses MSN Messenger to retrieve e-mail addresses. Without MSN Messenger, this worm just sends e-mail to:

- Sarah700@e-mail.com

The worm arrives as an attachment with the filename, SARAH.SCR. It has a destructive payload and deletes all files in the first level folder from the root directory and modifies certain critical files, preventing affected systems from restarting.

**Worm/P2P.Sambud.B (Alias: Worm/Hallo.B) (Internet Worm):** This worm uses the file exchange P2P network KaZaA to trick users into downloading itself. If executed, the worm copies itself in the \windows\system32\ directory under the filename "Spank_Britney.exe." It then creates a couple registry key entries so that it enables the KaZaA shared files and where to direct the shared folders, including:

- HKEY_CURRENT_USER\Software\Kazaa\LocalContent "dir99"="012345:C:\\WINDOWS\\sys32"

**Wyx.C (b) (Polymorphic Virus):** This is a polymorphic virus that infects boot sectors on local hard disks and floppy disks. It carries no payload, but may destroy FAT32 partitions when infecting them. Once activated, Wyx.C (b) reduces the total memory available to DOS applications by 2 KB and then loads itself at the top of memory (at the 638K limit). It then infects the Master Boot Record (MBR) and the Disk Boot Sector (DBS) of the first active partition on the local hard disk. It is a memory-resident virus that checks periodically for uninfected boot sectors (using the timer interrupt which is activated about 18.7 times per second) on any floppy disk in drive A or on the local hard disk (MBR or DBS of first active partition). Due to bugs in the virus it may:

- Overwrite part of the display memory during execution. This may cause garbled data to appear at the top of the screen.
- Damage or destroy FAT32 partitions when infecting them.

Wyx.C (b) contains the string:

- 20/01/2001 WYX

## *Trojans*

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| AIM-Flood | N/A | CyberNotes-2002-16 |
| APStrojan.sl | N/A | CyberNotes-2002-03 |
| Arial | N/A | CyberNotes-2002-08 |
| Backdoor.Anakha | N/A | CyberNotes-2002-13 |
| Backdoor.AntiLam | N/A | CyberNotes-2002-12 |
| Backdoor.Assasin | N/A | CyberNotes-2002-14 |
| **Backdoor.Cabro** | **N/A** | **Current Issue** |
| Backdoor.Crat | N/A | CyberNotes-2002-12 |
| Backdoor.Delf | N/A | CyberNotes-2002-16 |
| Backdoor.Delf.B | N/A | CyberNotes-2002-16 |
| **Backdoor.Delf.C** | **N/A** | **Current Issue** |
| Backdoor.Ducktoy | N/A | CyberNotes-2002-15 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| Backdoor.Easyserv | N/A | CyberNotes-2002-16 |
| Backdoor.EggHead | N/A | CyberNotes-2002-04 |
| Backdoor.Evilbot | N/A | CyberNotes-2002-09 |
| Backdoor.Fearic | N/A | CyberNotes-2002-16 |
| Backdoor.FTP_Bmail | N/A | CyberNotes-2002-12 |
| Backdoor.G_Door.Client | N/A | CyberNotes-2002-05 |
| Backdoor.GRM | N/A | CyberNotes-2002-13 |
| Backdoor.GSpot | N/A | CyberNotes-2002-12 |
| Backdoor.IISCrack.dll | N/A | CyberNotes-2002-04 |
| Backdoor.Kavar | N/A | CyberNotes-2002-16 |
| Backdoor.Latinus | N/A | CyberNotes-2002-12 |
| Backdoor.Mirab | N/A | CyberNotes-2002-13 |
| Backdoor.MLink | N/A | CyberNotes-2002-16 |
| **Backdoor.Ndad** | **N/A** | **Current Issue** |
| Backdoor.NetControle | N/A | CyberNotes-2002-13 |
| Backdoor.NetDevil | N/A | CyberNotes-2002-04 |
| Backdoor.Nota | N/A | CyberNotes-2002-12 |
| Backdoor.Omed.B | N/A | CyberNotes-2002-11 |
| **Backdoor.Osirdoor** | **N/A** | **Current Issue** |
| Backdoor.RemoteNC | N/A | CyberNotes-2002-09 |
| Backdoor.Sazo | N/A | CyberNotes-2002-13 |
| **Backdoor.Scanboot** | **N/A** | **Current Issue** |
| Backdoor.Sparta | N/A | CyberNotes-2002-13 |
| Backdoor.Subwoofer | N/A | CyberNotes-2002-04 |
| Backdoor.Surgeon | N/A | CyberNotes-2002-04 |
| Backdoor.Systsec | N/A | CyberNotes-2002-04 |
| **Backdoor.Tela** | **N/A** | **Current Issue** |
| Backdoor.Theef | N/A | CyberNotes-2002-15 |
| Backdoor.Tron | N/A | CyberNotes-2002-12 |
| Backdoor.Ultor | N/A | CyberNotes-2002-13 |
| Backdoor.WinShell | N/A | CyberNotes-2002-16 |
| **Backdoor.Y3KRat.15** | **N/A** | **Current Issue** |
| BackDoor-ABH | N/A | CyberNotes-2002-06 |
| BackDoor-ABN | N/A | CyberNotes-2002-06 |
| BackDoor-FB.svr.gen | N/A | CyberNotes-2002-03 |
| Banan.Trojan | N/A | CyberNotes-2002-15 |
| Bck/Litmus.201 | N/A | CyberNotes-2002-14 |
| BDS/ConLoader | N/A | CyberNotes-2002-12 |
| BDS/Osiris | N/A | CyberNotes-2002-06 |
| BKDR_EMULBOX.A | N/A | CyberNotes-2002-10 |
| BKDR_INTRUZZO.A | N/A | CyberNotes-2002-09 |
| BKDR_LITMUS.C | N/A | CyberNotes-2002-09 |
| BKDR_SMALLFEG.A | N/A | CyberNotes-2002-04 |
| BKDR_WARHOME.A | N/A | CyberNotes-2002-06 |
| **Cardst** | **N/A** | **Current Issue** |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| Dewin | N/A | CyberNotes-2002-08 |
| DoS-Winlock | N/A | CyberNotes-2002-03 |
| Downloader-W | N/A | CyberNotes-2002-08 |
| FakeGina.Trojan | N/A | CyberNotes-2002-16 |
| Fortnight | N/A | CyberNotes-2002-10 |
| **IIS.Beavuh-Exploit** | **N/A** | **Current Issue** |
| IRC.kierz | N/A | CyberNotes-2002-16 |
| Irc-Smallfeg | N/A | CyberNotes-2002-03 |
| IRC-Smev | N/A | CyberNotes-2002-08 |
| JS/NoClose | N/A | CyberNotes-2002-11 |
| Liquid.Trojan | N/A | CyberNotes-2002-14 |
| mIRC/Gif | N/A | CyberNotes-2002-08 |
| Multidropper-CX | N/A | CyberNotes-2002-08 |
| **Netbus.160.Dropper** | **N/A** | **Current Issue** |
| PWS-AOLFake | N/A | CyberNotes-2002-15 |
| **PWS-MSNSteal** | **N/A** | **Current Issue** |
| PWS-Ritter | N/A | CyberNotes-2002-16 |
| **PWSteal.Kaylo** | **N/A** | **Current Issue** |
| **PWSteal.Netsnake** | **N/A** | **Current Issue** |
| **PWSteal.Profman** | **N/A** | **Current Issue** |
| QDel227 | N/A | CyberNotes-2002-09 |
| QDel234 | N/A | CyberNotes-2002-11 |
| RCServ | N/A | CyberNotes-2002-10 |
| StartPage-B | N/A | CyberNotes-2002-16 |
| Swporta.Trojan | N/A | CyberNotes-2002-13 |
| TR/Win32.Rewin | N/A | CyberNotes-2002-12 |
| Tr/WiNet | N/A | CyberNotes-2002-10 |
| TR/Zirko | N/A | CyberNotes-2002-10 |
| **Troj/Apher-A** | **N/A** | **Current Issue** |
| Troj/Diablo | N/A | CyberNotes-2002-09 |
| Troj/DSS-A | N/A | CyberNotes-2002-12 |
| Troj/Flood-O | N/A | CyberNotes-2002-14 |
| Troj/ICQBomb-A | N/A | CyberNotes-2002-05 |
| Troj/Kbman | N/A | CyberNotes-2002-10 |
| Troj/Momma-B | N/A | CyberNotes-2002-11 |
| Troj/Msstake-A | N/A | CyberNotes-2002-03 |
| **Troj/Ritter-A** | **N/A** | **Current Issue** |
| Troj/Tobizan-A | N/A | CyberNotes-2002-16 |
| Troj/Unreal-A | N/A | CyberNotes-2002-16 |
| TROJ_DOAL.A | N/A | CyberNotes-2002-14 |
| TROJ_DSNX.A | N/A | CyberNotes-2002-03 |
| TROJ_ICONLIB.A | N/A | CyberNotes-2002-03 |
| TROJ_JUNTADOR.B | N/A | CyberNotes-2002-06 |
| TROJ_JUNTADOR.G | N/A | CyberNotes-2002-10 |
| TROJ_OPENME.B | N/A | CyberNotes-2002-09 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| TROJ_SMALL.J | N/A | CyberNotes-2002-10 |
| TROJ_SMALLFEG.DR | N/A | CyberNotes-2002-04 |
| TROJ_SQLSPIDA.B | N/A | CyberNotes-2002-11 |
| TROJ_WORTRON.10B | N/A | CyberNotes-2002-12 |
| **Trojan.Adnap** | **N/A** | **Current Issue** |
| Trojan.Allclicks.A | N/A | CyberNotes-2002-13 |
| Trojan.Beway | N/A | CyberNotes-2002-15 |
| **Trojan.Crabox** | **N/A** | **Current Issue** |
| Trojan.Fatkill | N/A | CyberNotes-2002-09 |
| Trojan.Junnan | N/A | CyberNotes-2002-16 |
| Trojan.Portacopo:br | N/A | CyberNotes-2002-16 |
| Trojan.Prova | N/A | CyberNotes-2002-10 |
| Trojan.PSW.CrazyBilets | N/A | CyberNotes-2002-12 |
| Trojan.PSW.M2 | N/A | CyberNotes-2002-13 |
| Trojan.Starfi | N/A | CyberNotes-2002-16 |
| **Trojan.Win32.MSNTrick** | **N/A** | **Current Issue** |
| VBS.Gascript | N/A | CyberNotes-2002-04 |
| VBS.Zevach | N/A | CyberNotes-2002-15 |
| VBS_CHICK.B | N/A | CyberNotes-2002-07 |
| VBS_THEGAME.A | N/A | CyberNotes-2002-03 |
| W32.Alerta.Trojan | N/A | CyberNotes-2002-05 |
| W32.Azak | N/A | CyberNotes-2002-16 |
| W32.Cbomb | N/A | CyberNotes-2002-16 |
| W32.Click | N/A | CyberNotes-2002-15 |
| W32.Delalot.B.Trojan | N/A | CyberNotes-2002-06 |
| W32.DSS.Trojan | N/A | CyberNotes-2002-09 |
| W32.Estrella | N/A | CyberNotes-2002-13 |
| W32.Evala.Worm | N/A | CyberNotes-2002-14 |
| W32.IRCBot | N/A | CyberNotes-2002-14 |
| W32.Kamil | N/A | CyberNotes-2002-16 |
| W32.Kotef | N/A | CyberNotes-2002-16 |
| W32.Libi | N/A | CyberNotes-2002-10 |
| W32.Maldal.J | N/A | CyberNotes-2002-07 |
| W32.Nuker.Winskill | N/A | CyberNotes-2002-15 |
| W32.Tendoolf | N/A | CyberNotes-2002-09 |
| W32.Wabbin | N/A | CyberNotes-2002-15 |
| WbeCheck | N/A | CyberNotes-2002-09 |
| Winshell | N/A | CyberNotes-2002-15 |

**Backdoor.Cabro:** This Trojan allows unauthorized access to the infected computer. It is a server that is used for backdoor access to a compromised computer. The port that is used for access is configured upon infection. It gathers configuration information, such as the registered owner, organization, product ID, and serial number. It also launches IRC bots if an IRC program is installed. When Backdoor.Cabro runs, it copies itself as %windir%\ASDAPI.exe and runs as a service.

**Backdoor.Delf.C:** This is a backdoor Trojan horse that allows unauthorized access to the infected computer. It also stops the processes of some antivirus and firewall software.

**Backdoor.Ndad:** This Trojan provides a graphical user interface to perform administrative tasks on a compromised Windows NT machine. It is an ASP-based utility that contains scripts to facilitate remote administrator access to a Windows NT-based computer. It allows a remote user to gather information about the computer, browse directories, change file attributes, read, write, and edit files, as well as run DOS commands directly through Cmd.exe. A remote malicious user can also upload files to, and send anonymous e-mail from the compromised computer. Backdoor.Ndad does not modify the system registry.

**Backdoor.Osirdoor (Aliases: Backdoor.Osirdoor.B, BKDR_OSIRDOOR.B, BackDoor-ABT):** This is a Backdoor Trojan that gives a malicious user unauthorized access to a compromised computer. When it is run, Backdoor.Osirdoor listens on port 56565 for a connection. Once connected, the malicious user is able to perform the following actions on a compromised computer: Perform a screen capture and transmit the images to the attacker; send keystrokes to other applications; play .mp3 files using the default mp3 player; display messages; and open and close the CD-ROM drive tray. The Trojan has access to the following resources of the compromised computer:

- File system
- Registry
- Printer

To activate itself at startup, Backdoor.Osirdoor creates the value, "Kernel32 <path to kernel32.exe>\kernel32.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

**Backdoor.Scanboot:** This Trojan allows unauthorized access to the infected computer. It is a server that is used for backdoor access to a compromised computer. When Backdoor.Scanboot runs, it does the following: iIt copies itself as C:\Windows\System\Scanboot.exe (the path is hard-coded) and listens on port 1533; and adds the value, "Scanboot  C:\windows\system\scanboot.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Run

so that the backdoor will run when you start Windows.

**Backdoor.Tela:** This is a backdoor Trojan horse that allows unauthorized access to the infected computer. When Backdoor.Tela runs, it copies itself as %windir%\Sttray32.exe. To cause itself to run when you start Windows, the Trojan creates the value, "Sttray32 %windir%\STTRAY32.EXE." in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

The Trojan then allows a malicious user to access the compromised system without authorization. This Trojan contains a component that permits the remote client to install an FTP server on the compromised computer.

**Backdoor.Y3KRat.15:** This is a backdoor Trojan horse that allows a malicious user to gain control of a compromised computer. When Backdoor.Y3KRat.15 runs, it does the following: it copies itself as %system%\Dcomcnofg.exe; and it also adds the value, "Dcomcnofg %SYSTEM%\Dcomcnofg.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that it runs each time that you start Windows. After Backdoor.Y3KRat.15 is installed, it notifies the client side using ICQ pager and establishes a connection with the malicious user through a password-protected authorization. The commands allow the malicious user to perform the following actions:

- Manage the installation of the backdoor
- Download and execute files
- Deliver system and network information to the malicious user, including login names and cached network passwords
- Intercept confidential information by hooking any keystrokes; intercept information that is displayed and submit it to the malicious user by means of a built-in SMTP server
- Install an FTP server, which allows the malicious user to use the compromised computer as a temporary storage device
- Alter many system parameters, such as screen resolution and system colors

- Perform other actions such as printing text; playing media files; opening or closing the CD-ROM drive; hiding things such as icons, the system tray, buttons, and the taskbar; switching the monitor off and on; and so forth

The Trojan tries to deactivate many antivirus programs. To hide its activity, it also tries to delete Netstat.exe.

**Cardst (Aliases: JS.Trojan.Cardst, Trojan.CardStealer, Trojan.AOL.HTML.Cardst, HTML_CARDST.A, JS/Card, JS.Cardsteal.Trojan):** This Trojan is written in JavaScript. It tries to convince the user that it is AOL Billing Center. The contents of the html page includes a form in which the user is asked to fill the details about his credit card, post address, phone numbers etc. Once this is done and the form submitted, the Trojan sends all the data to the virus writer.

**IIS.Beavuh-Exploit (Alias: Exploit.IIS.Beavuh):** This detection was originally created in an effort to detect code that is used for malicious purposes, such as executing code on an IIS server or gaining access by means of a buffer overflow. The IIS.Beavuh-Exploit exists in IIS 5.0 Servers on Windows 2000 systems. This exploit uses the Internet Printing Protocol Vulnerability, which can overrun the buffer and cause the Trojan code to execute and obtain control of the server in a manner that is similar to a backdoor Trojan. It is recommended that all IIS 5.0 users download the patch for this exploit from the Microsoft Web site at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-023.asp.

**Netbus.160.Dropper:** This Trojan drops components of W95.Netbus.160.Trojan onto the target system. Because it is a dropper, it might behave differently from one version to another. In some cases it does the following:

- Copies itself to the %windir% folder
- Drops %windir%\Keyhook.dll
- Sets itself to run on startup by adding the value <name of dropper without extension> %windir%\file name to the registry key:
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

**PWSteal.Kaylo (Aliases: Trojan.PSW.Kaylo, TROJ_PSW.KAYLO.A, PWS-Kaylo):** This is a password-stealing Trojan. It is a Delphi application that is packed with ASPack v1.02. The Trojan attempts to search through your cached passwords and submit them the author of the Trojan, whose e-mail domain is located in Russia. It relies on an officially undocumented function, WNetEnumCachedPasswords that exists only in Windows95/98/ME versions of the file Mpr.dll. It uses this function to obtain an access to the password cache that is stored on the local computer. The cached passwords include modem and dialup passwords, URL passwords, share passwords, and others. To enable itself to run at startup, the Trojan adds the value, "OsaRun <trojan filename>" to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

PWSteal.Kaylo searches all active RAS connections to retrieve the current state of the connection process. If it finds a successfully established connection, it composes and sends out an e-mail to the author of the Trojan, using its own SMTP engine.

**PWS-MSNSteal (Aliases: Trojan.PSW.Ravenpass.b, Trojan.Starfi):** This is an MSN Messenger password stealer Trojan. It was coded in Visual Basic 6, and requires MSVBVM60.DLL in order to run. The internal name of this Trojan is "DONT CLICK.exe." The file icon of this Trojan is misleading, and becomes even more unobtrusive on default installations of Windows, where extensions of known file types can be hidden.

**PWSteal.Netsnake:** This is a Trojan horse that steals passwords. It collects user passwords and mails them to the intruder. It copies itself to %windir%\Internat.exe. Please note that there is a legitimate Windows application called %windir%\system\Internat.exe. The Trojan file is 82.5 KB in length and uses a zip file icon. The "real" Internat.exe is generally about 20 KB in length with a "?" icon. After the Trojan copies itself, it adds the value, "Internat.exe %windir%\internat.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. When it runs at startup, it displays the message:

- Hello. I'm NetSnake.

**PWSteal.Profman (Aliases: Trojan.PSW.Profman, TROJ_PROFMAN.C, PWS-Profman):** This is a password-stealing Trojan that is packed with ASPack v1.08.03. The trojan attempts to steal the dial-up connection details from your computer and submit them to the author of the Trojan, whose e-mail domain is located in Russia. It then retrieves the following connection information saved by the last successful call:

- The phone number
- The user's user name
- The user's password that was used to authenticate the user's access to the remote access server

To enable itself to run at startup, the Trojan adds the value, ProfileManager "profman /CheckUserName /OleShared" to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

The stolen dial-up connection details are then submitted by e-mail to the author of the Trojan, using its own SMTP engine.

**Troj/Apher-A (Aliases: Apher, TrojanDownloader.Win32.Apher.gen, Backdoor.Death.25.gen):** This is a Trojan which will download and install Troj/Death-25-J. It is a backdoor Trojan. When run, the Trojan will copy itself to C:\windows\system\vbwinsok.exe and set the following registry keys to point to this file:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\vbwinsok.exe
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\vbwinsok.exe

It spreads in e-mail messages as follows:

- From:info@microsoft.com
- Subject:Protect Your NetWare with KasperskyTM Anti-
- VirusAttachment: AAPRICES.EXE

Once the attachment is executed, it downloads and silently executes from a Russian web site a file Slnew.exe. This file contains the mass mailing routine as well as a new variant of Backdoor.Death.25. The backdoor provides access to the compromised computer for any remote malicious user

**Troj/Ritter-A:** This is a password stealing Trojan for Novell networks. The Trojan can only be used against NetWare 3 servers (or servers with bindery emulation enabled) because it uses the bindery as a database to store the passwords it steals. It consists of two files. PROP.EXE must be run as SUPERVISOR to create the necessary storage area in the bindery and is also used later to retrieve stolen passwords. LOGIN.EXE is a modified version of the NetWare 3 login program that a malicious user must write over the genuine LOGIN.EXE in order to steal usernames and passwords as they are typed in.

**Trojan.Adnap:** This Trojan tries to spoof another vendor's antivirus program. When Trojan.Adnap runs, it uses TCP/IP port 20480 to connect to a Web page that is hosted by www.geocities.com. It adds the following line to the Autoexec.bat file:

- @copy <original Trojan file name> C:\Windows\FPanda.exe

The Trojan adds these values:

- APVXD C:\Windows\FPanda
- APVXDWin <original Trojan file name>

to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that it runs when you start Windows.

**Trojan.Crabox:** This is a Trojan horse that attempts to overload the play.mp3.com Web site by sending requests to it. The file name that this Trojan uses is Crackerbox.exe. When Trojan.Crabox runs, it immediately begins to send requests to play.mp3.com. The Trojan also adds itself to the Startup folder on the Windows Start menu. This causes the Trojan to run each time that Windows is started. Even though Trojan.Crabox does not cause any damage to the computer on which it runs, it does use a substantial amount of bandwidth. This results in slower connections to the Internet. Currently mp3.com will display a message if the Trojan successfully sent the request.

**Trojan.MSNTrick (Alias: Trojan.Win32.MSNTrick):** This is a Trojan horse that is written in Visual Basic. The Trojan steals passwords from MSN Messenger users. When the Trojan runs, it attempts to steal your MSN Messenger ID and password and send them to the Trojan's author. If you find this Trojan on your computer, you must change your MSN Messenger password as soon as possible.